REMARKS

Claims 1-3, 7-13, 16, 17, 20 and 26-29 stand rejected under 35 U.S.C. 102(e) as allegedly being anticipated by Flint et al. (US Patent 6,453,419). This contention is respectfully traversed.

Claims 6, 14, 15 and 18-20 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Flint et al. as applied to independent claim 1 and 17 above, in view of Green et al. (US Patent 6,003,084). This contention is respectfully traversed.

Claims 21-23 and 25 stand rejected under 35 U.S.C. 103(a) as allegedly being unpatentable over Flint et al. in further view of Green et al., in further view of Cunningham et al. (US Patent 6,219,786), in further view of Trcka et al. (US 6,453,345). This contention is respectfully traversed.

I. The Rejection under 35 U.S.C. 112

Claim 25 has been amended to correct the antecedent basis, thus rendering the rejection under 35 U.S.C. 112 moot.

II. The Rejections under 35 U.S.C. 102 and 103

The Office Action's Response to Arguments

First, with respect to the office action's response to arguments on page 12, it is respectfully noted that although

Flint does show a VPN, it does not teach or suggest the particular features of the claims, as outlined in detail below.

Second, with respect to the office action's assertion that Flint teaches the way the client gets policies in the way by teaching that access control is maintained through workstations through and internal and external network connections, it is respectfully noted that Flint teaches that access control lists are implemented in the firewall. Flint does teach network connections, servers, and the like, but does not teach the particular features of claim 1, as outlined below.

Claim 1

Claim 1 is rejected under 35 U.S.C. 102(e) as allegedly being anticipated by Flint. However, Flint neither teaches nor suggests the features of claim 1.

For example, Flint neither teaches nor suggests "delivering security policies from a server to a remote system," as recited in claim 1.

The office action cites column 2, lines 6-11 as teaching "delivering security policies," and alleges that "delivering" is the same as "providing."

The office action cites column 3, lines 3-7 as teaching "from a server to a remote system that has predetermined configuration information."

The office action improperly disregards the explicit language of claim 1. First, the word "providing" is not the same as the word "delivering." Although "delivering" security policies may be said to be one type of "providing" security policies (i.e., delivering may be said in some circumstances to be a species of the genus providing), the converse is not true.

In particular, the cited portion of Flint, column 2, lines 6-11, teaches "The present invention is a system and method of implementing a security policy, comprising the steps of providing a plurality of access policies, defining a process and connecting the access policies and the process to form a security policy." According to Flint, access control rules define the security policy (please see column 2, line 19 of Flint), and the access control rules are implemented in firewalls such as firewall 34 of FIG. 2.

Thus, there is no suggestion in Flint that security policies (in Flint, the access control rules) are delivered at all. Rather, the access control rules are applied by the firewall. Flint explains "ACLs are the heart and soul of firewall 34. For each connection attempt, the firewall checks the ACLs for permissions on use and for constraints for the connection." (Please see column 3, lines 45-56 of Flint).

Second, the office action improperly disregards the explicit language of claim 1 when it divorces the phrase "delivering security policies" from the phrase "from a server to a remote system that has predetermined configuration information." As noted above, Flint does not teach delivering security policies.

It certainly does not teach delivering security policies from a server to a remote system that has predetermined configuration information. The portion of Flint cited as teaching the "from a server…" feature of claim 30 merely describes system 30 of FIG. 1B. Although FIG. 1B does show a firewall 34, and servers 42 and 38, it does not teach that security policies are delivered from either server 42 and 38 to a remote system.

Claim 1 further recites "establishing a secure virtual private network connection between the server and the system." In Flint, VPN connections are shown between firewall 34 and partner shared network 46 in FIG. 2, and between firewall 34 and sales offices 46 in FIG. 3. Therefore, it appears that the office action is identifying firewall 34 as the server (or the remote system), and partner shared network 46 or sales office 46 as the remote system (or the server). Therefore, in order to teach the above feature of claim 1, security policies would need to be delivered from (to) firewall 34 to (from) network 46 or office 46. Flint does not so teach. As explained above, Flint teaches that the access control rules define the security policy (in column 2, lines 17-18), and that the access control rules are implemented at the firewall ("ACLs are the heart and soul of firewall 34," at column 3, line 54).

Since Flint neither teaches nor suggests these features, claim 30 is patentable over Flint. Further, it is not obvious to modify Flint to include features such as those in claim 30. First, there is no motivation in the references to do so. Second, such a modification would change the principle of operation of Flint (which is direct to a method of presenting and managing access control rules of a firewall), and is thus not obvious.

The motivation to provide the features of claim 30 comes from Applicant's specification alone. As noted in a previous response, an important feature of the present system is the way the client gets policies for secure connections over virtual private networks, and enforces the policies from the VPN over the network, in a special way.

Claim 1 is further patentable over Flint because Flint neither teaches nor suggests "regulating activities in the system based on both of the security policies and a context of said at least one application program including at least a state of running of said at least one application program," as recited in claim 1.

As noted in a previous response, Flint teaches that access rules are formed using decision trees allowing decisions to be made for criteria such as time of day or the like. However, there is no decision rule stated in Flint which teaches or suggests using the running state of an application program.

The office action asserts that this feature is taught in column 4, lines 14-26 of Flint. However, the cited feature of Flint does not so teach. Specifically, the teaching that "Also included are the system calls that the user level programs need to use the ACLs" (column 4, lines 17-19) is not a teaching that activities are regulated based on "a state of running of at least one application program." This portion merely teaches that the kernel code includes system calls for user level programs.

For at least the above reasons, claim 1 is patentable over Flint.

Claims 2, 3, 6-16

Claims 2, 3, 6-16 depend from claim 1 and are therefore patentable for at least the same reasons as stated above with respect to claim 1.

Claims 17-23 and 25-29

Independent claims 17 and 21 include features similar to claim 1 above, and are therefore patentable for at least the same reasons as stated above with respect to claim 1. Claims

18-20 and 22, 23, and 25-29 depend from claims 17 and 21, respectively, and are therefore patentable for at least the same reasons as stated above with respect to claims 17 and 21.

New Claims 30-34

New claims 30-34 have been added to clearly emphasize patentable features of the current disclosure. For example, new claims 30-34 detail the relationship between a primary computing system (which may be a corporate LAN) and a remote computing system (which may a remote home network) of a VPN, where a network stack of the remote computing system may be dynamically reconfigured. Claims 30-34 further detail of an implementation in which a word processing program is running or not running.

CONCLUSION

It is believed that all of the pending claims have been addressed in this paper. However, failure to address a specific rejection, issue, or comment, does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above are not intended to be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

In view of the above amendments and remarks, therefore, all of the claim should be in condition for allowance. A formal notice to that effect is respectfully solicited. If the Examiner has any questions regarding this response, the Examiner is invited to telephone the undersigned at (858) 678-5070.

Enclosed is a $176.00 check for excess claim fees. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: 09/14/04

Kenyon

Linda G. Gunderson
Reg. No. 46,341
Attorney for Intel Corporation

/BY
KENYON S. JENCKES
REG. NO. 41,873

Fish & Richardson P.C.
PTO Customer Number: **20985**
4350 La Jolla Village Drive, Suite 500
San Diego, CA 92122
Telephone: (858) 678-5070
Facsimile: (858) 678-5099
10426081.doc